

## TRAITE DE COOPERATION EN MATIERE DE BREVETS

PCT

## NOTIFICATION D'ELECTION

(règle 61.2 du PCT)

Expéditeur: le BUREAU INTERNATIONAL

Destinataire:

Commissioner  
 US Department of Commerce  
 United States Patent and Trademark  
 Office, PCT  
 2011 South Clark Place Room  
 CP2/5C24  
 Arlington, VA 22202  
 ETATS-UNIS D'AMERIQUE  
 en sa qualité d'office élu

Date d'expédition (jour/mois/année) 02 novembre 2000 (02.11.00)	
Demande internationale no PCT/FR00/00723	Référence du dossier du déposant ou du mandataire GEM0652
Date du dépôt international (jour/mois/année) 22 mars 2000 (22.03.00)	Date de priorité (jour/mois/année) 26 mars 1999 (26.03.99)
Déposant CORON, Jean-Sébastien	

1. L'office désigné est avisé de son élection qui a été faite:

☒ dans la demande d'examen préliminaire international présentée à l'administration chargée de l'examen préliminaire international le:

23 septembre 2000 (23.09.00)

☐ dans une déclaration visant une élection ultérieure déposée auprès du Bureau international le:

2. L'élection ☒ a été faite

☐ n'a pas été faite

avant l'expiration d'un délai de 19 mois à compter de la date de priorité ou, lorsque la règle 32 s'applique, dans le délai visé à la règle 32.2b).

Bureau international de l'OMPI 34, chemin des Colombettes 1211 Genève 20, Suisse no de télécopieur: (41-22) 740.14.35	Fonctionnaire autorisé Diana Nissen no de téléphone: (41-22) 338.83.38
--	--

# TRAITE DE COOPERATION EN MATIERE DE BREVETS

## PCT

### RAPPORT DE RECHERCHE INTERNATIONALE

(article 18 et règles 43 et 44 du PCT)

Référence du dossier du déposant ou du mandataire <b>GEM0652</b>	<b>POUR SUITE A DONNER</b> voir la notification de transmission du rapport de recherche internationale (formulaire PCT/ISA/220) et, le cas échéant, le point 5 ci-après	
Demande internationale n° <b>PCT/FR 00/ 00723</b>	Date du dépôt international(jour/mois/année) <b>22/03/2000</b>	(Date de priorité (la plus ancienne) (jour/mois/année) <b>26/03/1999</b>
Déposant <b>GEMPLUS et al.</b>		

Le présent rapport de recherche internationale, établi par l'administration chargée de la recherche internationale, est transmis au déposant conformément à l'article 18. Une copie en est transmise au Bureau international.

Ce rapport de recherche internationale comprend 2 feuilles.



Il est aussi accompagné d'une copie de chaque document relatif à l'état de la technique qui y est cité.

#### 1. Base du rapport

- a. En ce qui concerne la **langue**, la recherche internationale a été effectuée sur la base de la demande internationale dans la langue dans laquelle elle a été déposée, sauf indication contraire donnée sous le même point.



la recherche internationale a été effectuée sur la base d'une traduction de la demande internationale remise à l'administration.

- b. En ce qui concerne les **séquences de nucléotides ou d'acides aminés** divulguées dans la demande internationale (le cas échéant), la recherche internationale a été effectuée sur la base du listage des séquences :



contenu dans la demande internationale, sous forme écrite.



déposée avec la demande internationale, sous forme déchiffrable par ordinateur.



remis ultérieurement à l'administration, sous forme écrite.



remis ultérieurement à l'administration, sous forme déchiffrable par ordinateur.



La déclaration, selon laquelle le listage des séquences présenté par écrit et fourni ultérieurement ne vas pas au-delà de la divulgation faite dans la demande telle que déposée, a été fournie.



La déclaration, selon laquelle les informations enregistrées sous forme déchiffrable par ordinateur sont identiques à celles du listage des séquences présenté par écrit, a été fournie.

2. ☐ Il a été estimé que certaines revendications ne pouvaient pas faire l'objet d'une recherche (voir le cadre I).

3. ☐ Il y a absence d'unité de l'invention (voir le cadre II).

#### 4. En ce qui concerne le titre,



le texte est approuvé tel qu'il a été remis par le déposant.



Le texte a été établi par l'administration et a la teneur suivante:

#### 5. En ce qui concerne l'abrégé,



le texte est approuvé tel qu'il a été remis par le déposant



le texte (reproduit dans le cadre III) a été établi par l'administration conformément à la règle 38.2b). Le déposant peut présenter des observations à l'administration dans un délai d'un mois à compter de la date d'expédition du présent rapport de recherche internationale.

#### 6. La figure des dessins à publier avec l'abrégé est la Figure n°



suggérée par le déposant.



parce que le déposant n'a pas suggéré de figure.



parce que cette figure caractérise mieux l'invention.



Aucune des figures n'est à publier.

# RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale No

P 00/00723

## A. CLASSEMENT DE L'OBJET DE LA DEMANDE

CIB 7 H04L9/30

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

## B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)

CIB 7 H04L

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)

## C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie *	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	<p>PAUL KOCHER ET AL.: "Introduction to Differential Power Analysis and Related Attacks"</p> <p>RETRIEVED FROM INTERNET: &lt;URL: HTTP://WWW.CRYPTOGRAPHY.COM/DPA/TECHNICAL/INDEX.HTML&gt; ON 24 FEBRUARY 2000; AVAILABLE ON INTERNET SINCE 1998, pages 1-8, XP002132318</p> <p>San Francisco, CA, USA</p> <p>page 7 -page 8</p> <p style="text-align: center;">---</p> <p style="text-align: center;">-/--</p>	<p>1,2,6,7, 11,15</p>

☒ Voir la suite du cadre C pour la fin de la liste des documents

☐ Les documents de familles de brevets sont indiqués en annexe

\* Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée

2 juin 2000

Date d'expédition du présent rapport de recherche internationale

09/06/2000

Nom et adresse postale de l'administration chargée de la recherche internationale  
Office Européen des Brevets, P.B. 5818 Patentlaan 2  
NL - 2280 HV Rijswijk  
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,  
Fax: (+31-70) 340-3016

Fonctionnaire autorisé

Zucka, G

## C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	MENKUS B: "Two important data encryption structures reported broken in record times" EDPACS, JAN. 1999, AUERBACH PUBLICATIONS, USA, vol. 26, no. 7, pages 15-18, XP000884687 ISSN: 0736-6981 page 18 ----	1,2,6,7, 11,15
A	KOCHER P C: "Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems" ADVANCES IN CRYPTOLOGY - CRYPTO'96. 16TH ANNUAL INTERNATIONAL CRYPTOLOGY CONFERENCE. PROCEEDINGS, ADVANCES IN CRYPTOLOGY - CRYPTO '96, SANTA BARBARA, CA, USA, 18-22 AUG. 1996, pages 104-113, XP000626590 1996, Berlin, Germany, Springer-Verlag, Germany ISBN: 3-540-61512-1 page 110, dernier alinéa -page 112, alinéa 2 ----	1,2,6,7, 11,15
A	KOBLITZ N: "Elliptic curve cryptosystems" MATHEMATICS OF COMPUTATION, JAN. 1987, USA, vol. 48, no. 177, pages 203-209, XP000671098 ISSN: 0025-5718 page 203 -page 205 -----	1,6,11, 15

09/937397  
JC16 Rec'd PCT/PTO SEP 26 2001

REPLACED BY  
ART 34 AMOT

TRANSLATION OF ANNEX TO  
INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(to be substituted for corresponding pages of the application as published)

In this section, an enciphering algorithm based on an elliptical curve is described. This scheme is similar to the El Gamal enciphering scheme. A message  $m$  is enciphered as follows:

5        The cipher clerk chooses an integer  $k$  randomly and calculates the points  $k.P=(x_1, y_1)$  and  $k.Q=(x_2, y_2)$  on the curve, and the integer  $c = x_2 + m$ . The cipher of  $m$  is the triplet  $(x_1, y_1, c)$ .

10       The deciphering clerk, who possesses  $d$ , deciphers  $m$  by calculating:

$$(x'_2, y'_2) = d(x_1, y_1) \text{ and } m = c - x'_2$$

15       In order to effect the scalar multiplications necessary in the calculation methods described previously, several algorithms exist:

20       "Double and add" algorithm;  
       "Addition-subtraction" algorithm;  
       Algorithm with addition chains;  
       Algorithm with window;  
       Algorithm with signed representation.

25       This list is not exhaustive. The simplest algorithm and the one which is most used is the "double and add" algorithm. The "double and add" algorithm takes as its input a point  $P$  belonging to a given elliptical curve and an integer  $d$ . The integer  $d$  is denoted  $d = (d(t), d(t-1), \dots, d(0))$ , where  $(d(t), d(t-1), \dots, d(0))$  is the binary representation of  $d$ , with  $d(t)$

30

the most significant bit and  $d(0)$  the least significant bit. The algorithm returns as an output the point  $Q=d.P$ .

5 The "double and add" algorithm includes the following three steps:

- 1) Initialising the point  $Q$  with the value  $P$
- 2) For  $i$  ranging from  $t-1$  to  $0$ , executing:
  - 2a) Replacing  $Q$  with  $2Q$
  - 10 2b) If  $d(i)=1$  replacing  $Q$  with  $Q+P$
- 3) Returning  $Q$ .

15 It became clear that the implementation of a public key enciphering algorithm of the elliptical curve type on a smart card was vulnerable to attacks consisting of a differential analysis of current consumption making it possible to find the private deciphering key. These attacks are known as DPA attacks, the acronym for Differential Power Analysis.

20 The principle of these DPA attacks is based on the fact that the current consumption of the microprocessor executing the instructions varies according to the data item being manipulated.

25 In particular, when an instruction is manipulating a data item in which a particular bit is constant, where the value of the other bits may vary, analysis of the current consumption related to the instruction shows that the mean consumption of the instruction is not the same according to whether the

30 particular bit takes the value  $0$  or  $1$ . The attack of

the DPA type therefore makes it possible to obtain additional information on the intermediate data manipulated by the microprocessor of the card when a cryptographic algorithm is being executed. This  
5 additional information can in some cases reveal the private parameters of the deciphering algorithm, making the cryptographic system insecure.

In the remainder of this document a description is given of a method of DPA attack on an algorithm of  
10 the elliptical curve type performing an operation of the type consisting of the scalar multiplication of a point  $P$  by an integer  $d$ , the integer  $d$  being the secret key. This attack directly reveals the secret key  $d$ . It therefore seriously compromises the security of the  
15 implementation of elliptical curves on a smart card.

The first step of the attack is the recording of the current consumption corresponding to the execution of the "double and add" algorithm described previously for  $N$  distinct points  $P(1), \dots, P(N)$ . In an algorithm  
20 based on elliptical curves, the microprocessor of the smart card will perform  $N$  scalar multiplications  $d.P(1), \dots, d.P(N)$ .

For clarity of the description of the attack, the first step is to describe a method for obtaining the  
25 value of the bit  $d(t-1)$  of the secret key  $d$ , where  $(d(t), d(t-1), \dots, d(0))$  is the binary representation of  $d$ , with  $d(t)$  the most significant bit and  $d(0)$  the least significant bit. Next the description of an algorithm which makes it possible to find the value of  $d$  is  
30 given.



The points  $P(1)$  to  $P(N)$  are grouped together according to the value of the last bit of the abscissa of  $4.P$ , where  $P$  designates one of the points  $P(1)$  to  $P(N)$ . The first group consists of the points  $P$  such that the last bit of the abscissa of  $4.P$  is equal to 1. The second group consists of the points  $P$  such that the last bit of the abscissa of  $4.P$  is equal to 0. The mean of the current consumptions corresponding to each of the two groups is calculated, and the difference curve between these two means is calculated.

If the bit  $d(t-1)$  of  $d$  is equal to 0, then the scalar multiplication algorithm previously described calculates and stores in memory the value of  $4.P$ . This means that, when the algorithm is executed in a smart card, the microprocessor of the card will actually calculate  $4.P$ . In this case, in the first message group, the last bit of the data item manipulated by the microprocessor is always at 1, and in the second message group the last bit of the data item manipulated is always at 0. The mean of the current consumptions corresponding to each group is therefore different. There therefore appears, in the difference curve between the two means, a differential current consumption peak.

If on the other hand the bit  $d(t-1)$  of  $d$  is equal to 1, the exponentiation algorithm described previously does not calculate the point  $4.P$ . When the algorithm is executed by the smart card, the microprocessor therefore never manipulates the data item  $4.P$ . Therefore no differential consumption peak appears.

This method therefore makes it possible to determine the value of the bit  $d(t-1)$  of  $d$ .

The algorithm described in the following section is a generalisation of the previous algorithm. It makes it possible to determine the value of the secret key  $d$ :

The input is defined by  $N$  points denoted  $P(1)$  to  $P(N)$  corresponding to  $N$  calculations performed by the smart card, and the output by an integer  $h$ .

The said algorithm is implemented as follows in three steps.

- 1) Executing  $h=1$ ;
- 2) For  $i$  ranging from  $t-1$  to 1, executing:
  - 2)1) Classifying the points  $P(1)$  to  $P(N)$  according to the value of the last bit of the abscissa of  $(4 \cdot h) \cdot P$ ;
  - 2)2) Calculating the current consumption mean for each of the two groups;
  - 2)3) Calculating the difference between the two means;
  - 2)4) If the difference shows a differential consumption peak, doing  $h=h \cdot 2$ ; otherwise doing  $h=h \cdot 2 + 1$ ;
- 3) Returning  $h$ .

The above algorithm supplies an integer  $h$  such that  $d=2 \cdot h$  or  $d=2 \cdot h + 1$ . In order to obtain the value of  $d$ , it then suffices to test the two possible hypotheses.

The attack of the DPA type described therefore makes it possible to find the private key  $d$ .

5 The method of the invention consists of in devising of three countermeasures to guard against the DPA attack described above.

The method of the first countermeasure consists in calculating, from the private key  $d$  and the number of points  $N$  on the elliptical curve, a new deciphering integer  $d'$ , such that the deciphering of any enciphered  
10 message with  $d'$  gives the same result as with  $d$ .

In the case of a cryptographic algorithm based on the use of elliptical curves performing the operation  $Q=d.P$  where  $d$  is the private key and  $P$  a point on the curve, the calculation of  $Q=d.P$  is replaced by the  
15 following method in four steps:

- 1) Determining a security parameter  $s$ ; in practice  $s$  can be taken close to 30.
- 2) Drawing a random number  $k$  between 0 and  $2^s$ .
- 20 3) Calculating the integer  $d'=d+k.n$ .
- 4) Calculating  $Q=d'.P$ .

The method of the first countermeasure comprises two variants which relate to the updating of the  
25 integer  $d'$ . The first variant consists of the fact that a new deciphering integer  $d'$  is calculated at each new execution of the deciphering algorithm, according to the method described previously. The second variant consists of the fact that a counter is incremented at  
30 each new execution of the deciphering algorithm. When

this counter reaches a fixed value  $T$ , a new deciphering integer  $d'$  is calculated according to the method described previously, and the counter is reset to zero. In practice,  $T=16$  can be taken.

5           The method of the first countermeasure therefore makes the previously described DPA attack impossible by changing the deciphering integer  $d$ .

10           The method of the second countermeasure applies to the first class of curves previously described, that is to say the curves defined on the finite field  $GF(p)$  having as its equation  $y^2=x^3+ax+b$ . The method of the second countermeasure consists in using a random calculation modulus at each new execution. This random modulus is of the form  $p' = p \cdot r$  where  $r$  is a random  
15 integer. The scalar multiplication operation  $Q=d \cdot P$  performed in an algorithm based on an elliptical curve is then performed according to the following method in five steps:

20           1) Determining a security parameter  $s$ ; in practice,  $s$  can be taken to be close to the number 60.

            2) Drawing the random number  $r$  whose binary representation makes  $s$  bits.

            3) Calculating  $p' = p \cdot r$ .

25           4) Executing the scalar multiplication operation  $Q=d \cdot P$ , the operations being performed modulo  $p'$ .

            5) Performing the reduction operation modulo  $p$  of the coordinates of the point  $Q$ .

The method of the second countermeasure comprises two variants which relate to the updating of the integer  $r$ . The first variant consists of the fact that a new integer  $r$  is calculated at each new execution of the deciphering algorithm, according to the method described previously. The second variant consists of the fact that a counter is incremented at each new execution of the deciphering algorithm. When this counter reaches a fixed value  $T$ , a new integer  $r$  is calculated according to the method described previously, and the counter is reset to zero. In practice,  $T+16$  can be taken.

The method of the third countermeasure consists in "masking" the point  $P$  to which it is wished to apply the scalar multiplication algorithm by adding a random point  $R$  to it.

The method of scalar multiplication of a point  $P$  by an integer  $d$  according to  $Q=d.P$  comprises the following five steps:

- 1) Drawing a random point  $R$  on the curve.
- 2) Calculating  $P'=P+R$ .
- 3) Scalar multiplication operation  $Q'=d.P'$ .
- 4) Scalar multiplication operation  $S=d.R$ .
- 5) Calculating  $Q=Q' - S$ .

The method of the third countermeasure comprises three variants. The first variant consists of the fact that a counter is incremented at each new execution of the deciphering algorithm. When the deciphering

algorithm is first executed, the algorithm is executed according to the five-step method described above. As long as the counter has not reached the limit value T, steps 1 and 4 of the method described above are not executed, the points R and S keeping the values taken during the previous execution. When the counter reaches the limit value T, the deciphering algorithm is implemented according to the method described previously in five steps, and the counter is reset to zero. In practice, T=16 can be taken.

The second variant consists of the fact that the card initially has in memory two points on the elliptical curves such that  $S=d.R$ . Steps 1 and 4 of the previous deciphering algorithm are replaced by the following steps 1' and 4':

- 1') Replacing R with 2.R.
- 4') Replacing S with 2.S.

The third variant consists of a modification of the second variant characterised in that a counter is incremented at each new execution of the deciphering algorithm. When the deciphering algorithm is first executed, the algorithm is executed according to the five-step method of the second variant described above. As long as the counter has not reached a limit value T, steps 1' and 4' of the method described above are not executed, points r and S keeping the values taken during the previous execution. When the counter reaches a limit value T, the deciphering algorithm is

implemented according to the method previously described in five steps, and the counter is reset to zero. In practice,  $T=16$  can be taken.

5       The application of the above three countermeasure methods makes it possible to protect any cryptographic algorithm based on elliptical curves against the DPA attack described above. The three countermeasures presented are also compatible with each other: it is possible to apply to the RSA deciphering algorithm one,  
10       two or three of the countermeasures described.

## CLAIMS

1. A countermeasure method in an electronic component implementing a public key cryptography algorithm based on the use of elliptical curves consisting in calculating, using the private key  $d$  and the number of points  $n$  on the said elliptical curve, a new deciphering integer  $d'$  such that the deciphering of any enciphered message, by means of a deciphering algorithm, with  $d'$ , gives the same result as with  $d$ , by effecting the operation  $Q=d \cdot P$ ,  $P$  being a point on the curve, a method characterised in that it comprises four steps:

- 1) Determining a security parameter  $s$ ; in practice  $s$  can be taken close to 30.
- 2) Drawing a random number  $k$  between 0 and  $2^s$ .
- 3) Calculating the integer  $d'=d+k \cdot n$ .
- 4) Calculating  $Q=d' \cdot P$ .

20

2. A countermeasure method according to Claim 1, characterised in that a first variant consists of the fact that a new deciphering integer  $d'$  is calculated at each new execution of the deciphering algorithm.

3. A countermeasure method according to Claim 1, characterised in that a second variant consists of the fact that a counter is incremented at each new execution of the deciphering algorithm until a fixed value  $T$  is reached.



4. A countermeasure method according to Claim 3, characterised in that, once the value  $T$  has been reached, a new enciphering integer is calculated according to the method of Claim 1 and the counter is  
5 reset to zero.

5. A countermeasure method according to Claim 3, characterised in that the value  $T$  is equal to the integer 16.

6. A countermeasure method in an electronic  
10 component implementing a public key cryptography algorithm based on the use of elliptical curves defined on a finite field  $GF(p)$ ,  $p$  being a prime number, having as its equation  $y^2 = x^3 + ax + b$ , consisting in using a random calculation modulus at each new execution of the  
15 form  $p' = p * r$  where  $r$  is a random integer and having a point  $P$ , characterised in that the said method executes the scalar multiplication operation in five steps:

1) Determining a security parameter  $s$ ; in  
20 practice,  $s$  can be taken to be close to the number 60.

2) Drawing the random number  $r$  whose binary representation makes  $s$  bits.

3) Calculating  $p' = p * r$ .

4) Executing the scalar multiplication operation  
25  $Q = d.P$ , the operations being performed modulo  $p'$ .

5) Performing the reduction operation modulo  $p$  of the coordinates of the point  $Q$ .

7. A countermeasure method according to Claim 6, characterised in that a new integer is calculated at each new execution of the deciphering algorithm.

5 8. A countermeasure method according to Claim 6, characterised in that a counter is incremented at each new execution of the deciphering algorithm.

9. A countermeasure method according to Claim 8, characterised in that the counter is reset to zero when it has reached a value T.

10 10. A countermeasure method according to Claim 8 or Claim 9, characterised in that the value T is equal to sixteen.

11. A countermeasure method in an electronic component implementing a public key cryptography  
15 algorithm based on the use of elliptical curves consisting in calculating, using the private key d and the number of points n on the said elliptical curve, a new deciphering integer d' such that the deciphering of  
20 any enciphered message, by means of a deciphering algorithm, with d', gives the same result as with d, by performing the operation  $Q=d*P$ , P being a point on the curve to which the scalar multiplication algorithm is applied, adding to it a random point R by an integer d according to the equation  $Q=d*P$ , a method characterised  
25 in that it comprises the following five steps:

- 1) Drawing a random point R on the curve.
- 2) Calculating  $P'=P+R$ .
- 3) Scalar multiplication operation  $Q'=d.P'$ .
- 30 4) Scalar multiplication operation  $S=d.R$ .

5) Calculating  $Q=Q' - S$ .

12. A countermeasure method according to Claim 12, characterised in that a counter is incremented at each new execution of the deciphering algorithm up to a value T.

13. A countermeasure method according to Claim 12, characterised in that the counter is reset to zero once the value T has been reached.

14. A countermeasure method according to Claim 12, characterised in that a counter is incremented at each new execution of the deciphering algorithm up to a value T.

15. A countermeasure method according to Claim 11, characterised in that the elliptical curve has in memory two points such that  $S=d*R$ , steps 1 and 4 then being replaced by steps 1' and 4':

1') Replacing R with 2.R.

4') Replacing S with 2.S.

16. A countermeasure method according to Claim 15, characterised in that a counter is incremented at each new execution of the deciphering algorithm up to a value T.

17. A countermeasure method according to Claim 15, characterised in that a counter is incremented at each new execution of the deciphering algorithm up to a value T.

## RAPPORT D'EXAMEN PRELIMINAIRE INTERNATIONAL

(article 36 et règle 70 du PCT)



Référence du dossier du déposant ou du mandataire GEM0652	<b>POUR SUITE A DONNER</b> voir la notification de transmission du rapport d'examen préliminaire international (formulaire PCT/IPEA/416)	
Demande internationale n° PCT/FR00/00723	Date du dépôt international (jour/mois/année) 22/03/2000	Date de priorité (jour/mois/année) 26/03/1999
Classification internationale des brevets (CIB) ou à la fois classification nationale et CIB H04L9/30		
Déposant GEMPLUS et al.		

1. Le présent rapport d'examen préliminaire international, établi par l'administration chargée de l'examen préliminaire international, est transmis au déposant conformément à l'article 36.
2. Ce RAPPORT comprend 5 feuilles, y compris la présente feuille de couverture.  
  
☒ Il est accompagné d'ANNEXES, c'est-à-dire de feuilles de la description, des revendications ou des dessins qui ont été modifiées et qui servent de base au présent rapport ou de feuilles contenant des rectifications faites auprès de l'administration chargée de l'examen préliminaire international (voir la règle 70.16 et l'instruction 607 des Instructions administratives du PCT).

Ces annexes comprennent 17 feuilles.

3. Le présent rapport contient des indications relatives aux points suivants:

- I ☒ Base du rapport
- II ☐ Priorité
- III ☐ Absence de formulation d'opinion quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle
- IV ☐ Absence d'unité de l'invention
- V ☒ Déclaration motivée selon l'article 35(2) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration
- VI ☐ Certains documents cités
- VII ☐ Irrégularités dans la demande internationale
- VIII ☒ Observations relatives à la demande internationale

Date de présentation de la demande d'examen préliminaire internationale  23/09/2000	Date d'achèvement du présent rapport  28.06.2001
Nom et adresse postale de l'administration chargée de l'examen préliminaire international:   Office européen des brevets - P.B. 5818 Patentlaan 2 NL-2280 HV Rijswijk - Pays Bas Tél. +31 70 340 - 2040 Tx: 31 651 epo nl Fax: +31 70 340 - 3016	Fonctionnaire autorisé  Zucka, G  N° de téléphone +31 70 340 4026  

**RAPPORT D'EXAMEN  
PRÉLIMINAIRE INTERNATIONAL**

Demande internationale n° PCT/FR00/00723

**I. Base du rapport**

1. En ce qui concerne les **éléments** de la demande internationale (*les feuilles de remplacement qui ont été remises à l'office récepteur en réponse à une invitation faite conformément à l'article 14 sont considérées dans le présent rapport comme "initialement déposées" et ne sont pas jointes en annexe au rapport puisqu'elles ne contiennent pas de modifications (règles 70.16 et 70.17)*):

**Description, pages:**

1-5	version initiale			
6-17	reçue(s) le	12/03/2001	avec la lettre du	07/03/2001

**Revendications, N°:**

1-15	reçue(s) le	12/03/2001	avec la lettre du	07/03/2001
------	-------------	------------	-------------------	------------

2. En ce qui concerne la **langue**, tous les éléments indiqués ci-dessus étaient à la disposition de l'administration ou lui ont été remis dans la langue dans laquelle la demande internationale a été déposée, sauf indication contraire donnée sous ce point.

Ces éléments étaient à la disposition de l'administration ou lui ont été remis dans la langue suivante: , qui est :

- ☐ la langue d'une traduction remise aux fins de la recherche internationale (selon la règle 23.1(b)).
- ☐ la langue de publication de la demande internationale (selon la règle 48.3(b)).
- ☐ la langue de la traduction remise aux fins de l'examen préliminaire internationale (selon la règle 55.2 ou 55.3).

3. En ce qui concerne les **séquences de nucléotides ou d'acide aminés** divulguées dans la demande internationale (le cas échéant), l'examen préliminaire internationale a été effectué sur la base du listage des séquences :

- ☐ contenu dans la demande internationale, sous forme écrite.
- ☐ déposé avec la demande internationale, sous forme déchiffrable par ordinateur.
- ☐ remis ultérieurement à l'administration, sous forme écrite.
- ☐ remis ultérieurement à l'administration, sous forme déchiffrable par ordinateur.
- ☐ La déclaration, selon laquelle le listage des séquences par écrit et fourni ultérieurement ne va pas au-delà de la divulgation faite dans la demande telle que déposée, a été fournie.
- ☐ La déclaration, selon laquelle les informations enregistrées sous déchiffrable par ordinateur sont identiques à celles du listage des séquences Présenté par écrit, a été fournie.

4. Les modifications ont entraîné l'annulation :

- ☐ de la description, pages :

**RAPPORT D'EXAMEN  
PRÉLIMINAIRE INTERNATIONAL**

Demande internationale n° PCT/FR00/00723

- ☐ des revendications, n°s :  
☐ des dessins, feuilles :

5. ☐ Le présent rapport a été formulé abstraction faite (de certaines) des modifications, qui ont été considérées comme allant au-delà de l'exposé de l'invention tel qu'il a été déposé, comme il est indiqué ci-après (règle 70.2(c)) :

*(Toute feuille de remplacement comportant des modifications de cette nature doit être indiquée au point 1 et annexée au présent rapport)*

6. Observations complémentaires, le cas échéant :

**V. Déclaration motivée selon l'article 35(2) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration**

**1. Déclaration**

Nouveauté	Oui : Revendications 1-15 Non : Revendications
Activité inventive	Oui : Revendications Non : Revendications 1-15
Possibilité d'application industrielle	Oui : Revendications 1-15 Non : Revendications

**2. Citations et explications  
voir feuille séparée**

**VIII. Observations relatives à la demande internationale**

Les observations suivantes sont faites au sujet de la clarté des revendications, de la description et des dessins et de la question de savoir si les revendications se fondent entièrement sur la description :  
**voir feuille séparée**

**Concernant le point V**

1. Il est fait référence aux documents suivants:

**D1: Paul Kocher et al.: 'Introduction to Differential Power Analysis and Related Attacks' <URL: <http://www.cryptography.com/dpa/technical/index.html>>, pages 1-8, XP002132318 San Francisco, CA, USA**

**D2: Menkus B: 'Two important data encryption structures reported broken in record times' EDPACS, Jan. 1999, Auerbach Publications, USA, vol. 26, no. 7, pages 15-18, XP000884687 ISSN: 0736-6981**

2. Le document D2 (Menkus) divulgue l'idée qui est à la base des revendications indépendantes. En effet, ce document divulgue (voir en particulier la page 18) un procédé de contre-mesure qui repose sur l'incorporation de calculs aléatoires dans le logiciel de la puce intégrée, ou sur la modification de l'ordre d'opérations effectuées par ce logiciel.

Le fait que dans les revendications indépendantes 1, 6, et 11 ces calculs aléatoires soient mis en oeuvre dans le cadre d'algorithmes à courbes elliptiques, en eux-mêmes bien connus, n'apporte aucun avantage qui irait au delà de cette idée de base, et cette caractéristique, bien que rendant nouveau l'objet de ces revendications, ne témoigne donc pas d'une activité inventive.

3. Vu que l'objet des revendications indépendantes est nouveau, ceci est également vrai pour les revendications dépendantes. Cependant, ces revendications ne contiennent pas de caractéristiques additionnelles qui rendent inventif leur objet.
4. Il est à noter que le document D1 est également considéré comme très pertinent.

**Concernant le point VIII**

L'utilisation de l'expression "une première variante consiste en ce que" dans la revendication 2, et "une seconde variante consiste en ce que" dans la revendication 3, rend ambigu l'objet de ces revendications (article 6 PCT).



Ces algorithmes sont facilement transposables aux courbes elliptiques. Ainsi, il est possible de mettre en œuvre des algorithmes assurant l'authentification, la confidentialité, le  
5 contrôle d'intégrité et l'échange de clé.

Un point commun à la plupart des algorithmes cryptographiques basés sur les courbes elliptiques est qu'ils comprennent comme  
10 paramètre une courbe elliptique définie sur un corps fini et un point  $P$  appartenant à cette courbe elliptique. La clé privée est un entier  $d$  choisi aléatoirement. La clef publique est un point de la courbe  $Q$  tel que  $Q=d.P$ . Ces  
15 algorithmes cryptographiques font généralement intervenir une multiplication scalaire dans le calcul d'un point  $R=d.T$  où  $d$  est la clef secrète.

20 Dans ce paragraphe, on décrit un algorithme de chiffrement à base de courbe elliptique. Un document Menkus B : " Two important data encryption structures reported broken in record times " EDPACS, Jan. 1999, auerbach  
25 Publications, USA, vol.26, no.7, pages 15-18, XP000884687 ISSN : 0736-6981, cité D2, suggère l'utilisation de nombres aléatoires sans préciser la mise en œuvre de ces nombres aléatoires dans le cadre d'algorithme à courbes  
30 elliptiques. Le schéma de cet alogrithme est analogue au schéma de chiffrement d'El Gamal. Un message  $m$  est chiffré de la manière suivante :

Le chiffreur choisit un entier  $k$  aléatoirement et calcule les points  $k.P=(x_1,y_1)$  et  $k.Q=(x_2,y_2)$  de la courbe, et l'entier  $c = x_2 + m$ . Le chiffré de  $m$  est le triplet  $(x_1,y_1,c)$ .

Le déchiffreur qui possède  $d$  déchiffre  $m$  en calculant :

$$(x'_2,y'_2)=d(x_1,y_1) \text{ et } m=c-x'_2$$

Pour réaliser les multiplications scalaires nécessaires dans les procédé de calcul décrits précédemment, plusieurs algorithmes existent :

Algorithme " double and add " ;

Algorithme " addition-soustraction "

Algorithme avec chaînes d'addition ;

Algorithme avec fenêtre ;

Algorithme avec représentation signée ;

Cette liste n'est pas exhaustive. L'algorithme le plus simple et le plus utilisé est l'algorithme " double and add ". L'algorithme " double and add " prend en entrée un point  $P$  appartenant à une courbe elliptique donnée et un entier  $d$ . L'entier  $d$  est noté  $d=(d(t),d(t-1),\dots,d(0))$ , où  $(d(t),d(t-1),\dots,d(0))$  est la représentation binaire de  $d$ , avec  $d(t)$  le bit de poids fort et  $d(0)$  le bit de poids faible. L'algorithme retourne en sortie le point  $Q=d.P$ .

L'algorithme " double and add " comporte les 3 étapes suivantes :

1) Initialiser le point  $Q$  avec la valeur  $P$

2) Pour  $i$  allant de  $t-1$  à  $0$  exécuter :

2a) Remplacer  $Q$  par  $2Q$

5 2b) Si  $d(i)=1$  remplacer  $Q$  par  $Q+P$

3) Retourner  $Q$ .

Il est apparu que l'implémentation sur carte à puce d'un algorithme de chiffrement à clé publique du type courbe elliptique était vulnérable à des attaques consistant en une analyse différentielle de consommation de courant permettant de retrouver la clé privée de déchiffrement. Ces attaques sont appelées  
15 attaques DPA, acronyme pour Differential Power Analysis. Le principe de ces attaques DPA repose sur le fait que la consommation de courant du microprocesseur exécutant des instructions varie selon la donnée manipulée.

20

En particulier, lorsqu'une instruction manipule une donnée dont un bit particulier est constant, la valeur des autres bits pouvant varier, l'analyse de la consommation de courant liée à  
25 l'instruction montre que la consommation moyenne de l'instruction n'est pas la même suivant que le bit particulier prend la valeur  $0$  ou  $1$ . L'attaque de type DPA permet donc d'obtenir des informations supplémentaires sur les données  
30 intermédiaires manipulées par le microprocesseur de la carte lors de l'exécution d'un algorithme cryptographique. Ces informations

supplémentaires peuvent dans certain cas permettre de révéler les paramètres privés de l'algorithme de déchiffrement, rendant le système cryptographique non sûr.

5

Dans la suite de ce document on décrit un procédé d'attaque DPA sur un algorithme de type courbe elliptique réalisant une opération du type multiplication scalaire d'un point  $P$  par un entier  $d$ , l'entier  $d$  étant la clé secrète. Cette  
10 attaque permet de révéler directement la clé secrète  $d$ . Elle compromet donc gravement la sécurité de l'implémentation de courbes elliptiques sur une carte à puce.

15

Le document Paul Kocher et al. : « Introduction to Differential Power Analysis and Related Attacks » <URL :

<http://www.cryptography.com/dpa/technical/index.html>>, pages

20 1-8, XP002132318 San Francisco, CA, USA, cité D1, suggère l'utilisation de contre-attaques dans des implémentations du type Diffie-Hellman, RSA ? DSS et autres systèmes sans jamais proposer de mises en œuvres précises.

25 La première étape de l'attaque est l'enregistrement de la consommation de courant correspondant à l'exécution de l'algorithme " double and add " décrit précédemment pour  $N$  points distincts  $P(1), \dots, P(N)$ . Dans un  
30 algorithme à base de courbes elliptiques, le microprocesseur de la carte à puce va effectuer  $N$  multiplications scalaires  $d.P(1), \dots, d.P(N)$ .

Pour la clarté de la description de l'attaque, on commence par décrire une méthode permettant d'obtenir la valeur du bit  $d(t-1)$  de la clé secrète  $d$ , où  $(d(t), d(t-1), \dots, d(0))$  est la représentation binaire de  $d$ , avec  $d(t)$  le bit de poids fort et  $d(0)$  le bit de poids faible. On donne ensuite la description d'un algorithme qui permet de retrouver la valeur de  $d$ .

10

On groupe les points  $P(1)$  à  $P(N)$  suivant la valeur du dernier bit de l'abscisse de  $4.P$ , où  $P$  désigne un des points  $P(1)$  à  $P(N)$ . Le premier groupe est constitué des points  $P$  tels que le dernier bit de l'abscisse de  $4.P$  est égal à 1. Le second groupe est constitué des points  $P$  tels que le dernier bit de l'abscisse de  $4.P$  est égal à 0. On calcule la moyenne des consommations de courant correspondant à chacun des deux groupes, et on calcule la courbe de différence entre ces deux moyennes.

20

Si le bit  $d(t-1)$  de  $d$  est égal à 0, alors l'algorithme de multiplication scalaire précédemment décrit calcule et met en mémoire la valeur de  $4.P$ . Cela signifie que lors de l'exécution de l'algorithme dans une carte à puce, le microprocesseur de la carte va effectivement calculer  $4.P$ . Dans ce cas, dans le premier groupe de message le dernier bit de la donnée manipulée par le microprocesseur est toujours à 1, et dans le deuxième groupe de

25

30

message le dernier bit de la donnée manipulée est toujours à 0. La moyenne des consommations de courant correspondant à chaque groupe est donc différente. Il apparaît donc dans la courbe de différence entre les 2 moyennes un pic de différentiel de consommation de courant.

Si au contraire le bit  $d(t-1)$  de  $d$  est égal à 1, l'algorithme d'exponentiation décrit précédemment ne calcule pas le point 4.P. Lors de l'exécution de l'algorithme par la carte à puce, le microprocesseur ne manipule donc jamais la donnée 4.P. Il n'apparaît donc pas de pic de différentiel de consommation.

15

Cette méthode permet donc de déterminer la valeur du bit  $d(t-1)$  de  $d$ .

L'algorithme décrit dans le paragraphe suivant est une généralisation de l'algorithme précédant. Il permet de déterminer la valeur de la clé secrète  $d$  :

20

On définit l'entrée par  $N$  points notés  $P(1)$  à  $P(N)$  correspondant à  $N$  calculs réalisés par la carte à puce et la sortie par un entier  $h$ .

25

Ledit algorithme s'effectue de la manière suivante en trois étapes.

30

- 1) Exécuter  $h=1$  ;
- 2) Pour  $i$  allant de  $t-1$  à 1, exécuter :

- 2)1) Classer les points  $P(1)$  à  $P(N)$  suivant la valeur du dernier bit de l'abscisse de  $(4 \cdot h) \cdot P$  ;
- 2)2) Calculer la moyenne de consommation de courant pour chacun des deux groupes ;
- 2)3) Calculer la différence entre les 2 moyennes ;
- 2)4) Si la différence fait apparaître un pic de différentiel de consommation, faire  $h = h \cdot 2$  ;  
10 sinon faire  $h = h \cdot 2 + 1$  ;
- 3). Retourner  $h$ .

L'algorithme précédent fournit un entier  $h$  tel que  $d = 2 \cdot h$  ou  $d = 2 \cdot h + 1$ . Pour obtenir la valeur de  
15  $d$ , il suffit ensuite de tester les deux hypothèses possibles.

L'attaque de type DPA décrite permet donc de retrouver la clé privée  $d$ .

20 Le procédé de l'invention consiste en l'élaboration de trois contre-mesures permettant de se prémunir contre l'attaque DPA précédemment décrite.

25 Le procédé de la première contre-mesure consiste à calculer à partir de la clé privée  $d$  et du nombre de points  $n$  de la courbe elliptique un nouvel entier de déchiffrement  $d'$ , tel que le déchiffrement d'un message chiffré quelconque  
30 avec  $d'$  donne le même résultat qu'avec  $d$ .

Dans le cas d'un algorithme cryptographique basé sur l'utilisation de courbes elliptiques réalisant l'opération  $Q=d.P$  où  $d$  est la clé privée et  $P$  un point de la courbe, le calcul de  $Q=d.P$  est remplacé par le procédé suivant en quatre étapes:

1) Détermination d'un paramètre de sécurité  $s$ , dans la pratique on peut prendre  $s$  voisin de 30.

2) Tirage d'un nombre aléatoire  $k$  compris entre 0 et  $2^s$ ;

3) Calcul de l'entier  $d'=d+k.n$ ;

4) Calcul de  $Q=d'.P$ .

Le procédé de la première contre-mesure comprend deux variantes qui concernent la mise à jour de l'entier  $d'$ . La première variante consiste en ce qu'un nouvel entier de déchiffrement  $d'$  est calculé à chaque nouvelle exécution de l'algorithme de déchiffrement, selon le procédé décrit précédemment. La seconde variante consiste en ce qu'un compteur est incrémenté à chaque nouvelle exécution de l'algorithme de déchiffrement. Lorsque ce compteur atteint une valeur fixée  $T$ , un nouvel entier de déchiffrement  $d'$  est calculé selon le procédé décrit précédemment, et le compteur est remis à zéro. Dans la pratique, on peut prendre  $T=16$ .



Le procédé de la première contre-mesure rend donc l'attaque DPA précédemment décrite impossible en changeant d'entier  $d$  de déchiffrement.

5

Le procédé de la deuxième contre-mesure s'applique à la première classe de courbes précédemment décrites, c'est à dire les courbes définies sur le corps fini  $GF(p)$  ayant pour  
10 équation  $y^2 = x^3 + ax + b$ . Le procédé de la deuxième contre-mesure consiste à utiliser un module de calcul aléatoire à chaque nouvelle exécution. Ce module aléatoire est de la forme  $p' = p * r$  où  $r$  est un entier aléatoire. L'opération de  
15 multiplication scalaire  $Q = d.p$  réalisée dans un algorithme à base de courbe elliptique s'effectue alors selon le procédé suivant en cinq étapes:

- 20 1) Détermination d'un paramètre de sécurité  $s$ ; dans la pratique, on peut prendre  $s$  voisin du nombre 60;
- 2) Tirage du nombre aléatoire  $r$  dont la représentation binaire fait  $s$  bits;
- 25 3) Calcul de  $p' = p * r$ ;
- 4) Exécuter l'opération de multiplication scalaire  $Q = d.P$ , les opérations étant effectuées modulo  $p'$ ;
- 5) Effectuer l'opération de réduction modulo  $p$   
30 des coordonnées du point  $Q$ .

Le procédé de la seconde contre-mesure comprend deux variantes qui concernent la mise à jour de l'entier  $r$ . La première variante consiste en ce qu'un nouvel entier  $r$  est calculé à chaque  
5 nouvelle exécution de l'algorithme de déchiffrement, selon le procédé décrit précédemment. La seconde variante consiste en ce qu'un compteur est incrémenté à chaque nouvelle exécution de l'algorithme de déchiffrement.  
10 Lorsque ce compteur atteint une valeur fix "e T, un nouvel entier  $r$  est calculé selon le procédé décrit précédemment, et le compteur est remis à zéro.. Dans la pratique, on peut prendre  $T+16$ .

15 Le procédé de la troisième contre-mesure consiste à " masquer " le point  $P$  sur lequel on veut appliquer l'algorithme de multiplication scalaire en lui ajoutant un point aléatoire  $R$ . Le procédé de multiplication scalaire d'un point  
20  $P$  par un entier  $d$  suivant  $Q=d.P$  comprend les cinq étapes suivantes:

- 1) Tirage d'un point aléatoire  $R$  sur la courbe;
- 25 2) Calcul de  $P' = P + R$ ;
- 3) Opération de multiplication scalaire  $Q' = d.P'$ ;
- 4) Opération de multiplication scalaire  $S = d.R$ ;
- 30 5) Calcul de  $Q = Q' - S$ .

Le procédé de la troisième contre-mesure comprend trois variantes. la première variante consiste en ce qu'un compteur est incrémenté à chaque nouvelle exécution de l'algorithme de  
5 déchiffrement. Lors de la première exécution de l'algorithme de déchiffrement, l'algorithme est exécuté suivant le procédé en cinq étapes décrit précédemment. Tant que le compteur n'a pas atteint la valeur limite  $T$ , les étapes 1 et 4 du  
10 procédé décrit précédemment ne sont pas exécutées, les points  $R$  et  $S$  gardant les valeurs prises lors de l'exécution précédente. Lorsque le compteur atteint la valeur limite  $T$ , l'algorithme de déchiffrement s "effectue  
15 suivant le procédé décrit précédemment en cinq étapes, et le compteur est remis à zéro. Dans la pratique, on peut prendre  $T=16$ .

La deuxième variante consiste en ce que la carte  
20 possède initialement en mémoire deux points de la courbe elliptique tels que  $S=d.R$ . Les étapes 1 et 4 de l'algorithme de déchiffrement précédent sont remplacées par les étapes 1' et 4' suivantes:

25 1') Remplacer  $R$  par  $2.R$ :

4') Remplacer  $S$  par  $2.S$ .

30 La troisième variante consiste en une modification de la deuxième variante caractérisée en ce qu'un compteur est incrémenté

à chaque nouvelle exécution de l'algorithme de déchiffrement. Lors de la première exécution de l'algorithme de déchiffrement, l'algorithme est exécuté suivant le procédé en cinq étapes de la  
5 deuxième variante décrit précédemment. Tant que le compteur n'a pas atteint une valeur limite T, les étapes 1' et 4' du procédé décrit précédemment ne sont pas exécutées, les points R et S gardant les valeurs prises lors de  
10 l'exécution précédente. Lorsque le compteur atteint une valeur limite T, l'algorithme de déchiffrement s'effectue suivant le procédé précédemment décrit en cinq étapes, et le compteur est remis à zéro. Dans la pratique, on  
15 peut prendre  $T=16$ .

L'application des trois procédés de contre-mesure précédents permet de protéger tout l'algorithme cryptographique basé sur les  
20 courbes elliptiques contre l'attaque DPA précédemment décrit. Les trois contre-mesures présentées sont de plus compatibles entre elles: il est possible d'appliquer à l'algorithme de déchiffrement RSA une, deux ou trois des contre-  
25 mesures décrites.

1- Procédé de contre-mesure dans un composant électronique mettant en oeuvre un algorithme de cryptographie à clé publique basé sur l'utilisation des courbes elliptiques consistant  
30 à calculer à partir de la clé privée d et du nombre de points n de ladite courbe elliptique

un nouvel entier de déchiffrement  $d'$  tel que le déchiffrement d'un message chiffré quelconque, au moyen d'un algorithme de déchiffrement, avec  $d'$  donne le même résultat qu'avec  $d$ , en réalisant  
5 l'opération  $Q=d \cdot P$ ,  $P$  étant un point de la courbe, procédé caractérisé en ce qu'il comprend quatre étapes:

1) Détermination d'un paramètre de sécurité  $s$ ,  
10 dans la pratique on peut prendre  $s$  voisin de 30;  
2) Tirage d'un nombre aléatoire  $k$  compris entre 0 et  $2^s$ ;

3) Calcul de l'entier  $d'=d+k \cdot n$ ;

15

4) Calcul de  $Q=d' \cdot P$ .

2- Procédé de contre-mesure selon la revendication 1 caractérisé en ce qu'une  
20 première variante consiste en ce qu'un nouvel entier de déchiffrement  $d'$  est calculé à chaque nouvelle exécution de l'algorithme de déchiffrement.

25 3- Procédé de contre-mesure selon la revendication 1 caractérisé en ce qu'une seconde variante consiste en ce qu'un compteur est incrémenté à chaque nouvelle exécution de l'algorithme de déchiffrement jusqu'à atteindre

une valeur fixée T.

4- Procédé de contre-mesure selon la revendication 3 caractérisé en ce qu'une fois la  
5 valeur T atteinte, un nouvel entier de chiffrement est calculé selon le procédé de la revendication 1 et le compteur est remis à zéro.

5- Procédé de contre-mesure selon la revendication 3 caractérisé la valeur T est  
10 égale à l'entier seize.

6- Procédé de contre-mesure dans un composant électronique mettant en oeuvre un algorithme de  
15 cryptographie à clé publique basé sur l'utilisation des courbes elliptiques définies sur un corps fini  $GF(p)$ ,  $p$  étant un nombre premier, ayant pour équation  $y^2 = x^3 + ax + b$ , consistant à utiliser un module de calcul  
20 aléatoire à chaque nouvelle exécution de la forme  $p' = p * r$  où  $r$  est un entier aléatoire et présentant un point  $P$  caractérisé en ce que ledit procédé exécute l'opération de multiplication scalaire en cinq étapes:

25 1) Détermination d'un paramètre de sécurité  $s$ ; dans la pratique, on peut prendre  $s$  voisin du nombre 60;

30 2) Tirage du nombre aléatoire  $r$  dont la représentation binaire fait  $s$  bits;

3) Calcul de  $p' = p * r$ ;

4) Exécuter l'opération de multiplication scalaire  $Q=d.P$ , les opérations étant effectuées modulo  $p'$ ;

5) Effectuer l'opération de réduction modulo  $p$   
5 des coordonnées du point  $Q$ .

7- Procédé de contre-mesure selon la revendication 6 caractérisé en ce qu'un nouvel entier est calculé à chaque nouvelle exécution  
10 de l'algorithme de déchiffrement.

8- Procédé de contre-mesure selon la revendication 6 caractérisé en ce qu'un compteur est incrémenté à chaque nouvelle exécution de  
15 l'algorithme de déchiffrement.

9- Procédé de contre-mesure selon la revendication 8 caractérisé en ce que le compteur est remis à zéro lorsqu'il a atteint  
20 une valeur  $T$ .

10- Procédé de contre-mesure selon la revendication 8 ou la revendication 9 caractérisé en ce que la valeur  $T$  est égale à  
25 seize.

11. Procédé de contre-mesure dans un composant électronique mettant en oeuvre un algorithme de cryptographie à clé publique basé sur  
30 l'utilisation des courbes elliptiques consistant à calculer à partir de la clé privée  $d$  et du nombre de points  $n$  de ladite courbe elliptique

un nouvel entier de déchiffrement  $d'$  tel que le  
déchiffrement d'un message chiffré quelconque,  
au moyen d'un algorithme de déchiffrement, avec  $d'$   
donne le même résultat qu'avec  $d$ , en réalisant  
5 l'opération  $Q=d*P$ ,  $P$  étant un point de la courbe  
sur lequel est appliqué l'algorithme de  
multiplication scalaire en lui ajoutant un point  
aléatoire  $R$  par un entier  $d$  suivant l'équation  
 $Q=d*P$ , procédé caractérisé en ce qu'il comprend  
10 cinq étapes suivantes:

- 1) Tirage d'un point aléatoire  $R$  sur la courbe;
- 2) Calcul de  $P'=P+R$ ;
- 15 3) Opération de multiplication scalaire  $Q'=d.P'$ ;
- 4) Opération de multiplication scalaire  $S=d.R$ ;
- 20 5) Calcul de  $Q=Q'-S$ .

12- Procédé de contre-mesure selon la  
revendication 11 caractérisé en ce qu'un  
compteur est incrémenté à chaque nouvelle  
25 exécution de l'algorithme de déchiffrement  
jusqu'à une valeur  $T$ .

13- Procédé de contre-mesure selon la  
revendication 12 caractérisé en ce que le  
30 compteur est remis à zéro une fois atteint la  
valeur  $T$ .



14- Procédé de contre-mesure selon la revendication 11 caractérisé en ce que la courbe elliptique possède en mémoire deux points tels que  $S=d \cdot R$ , les étapes 1 et 4 étant alors  
5 remplacé par les étapes 1' et 4':

1') Remplacer R par 2.R:

4') Remplacer S par 2.S.

10

15- Procédé de contre-mesure selon la revendication 14 caractérisé en ce qu'un compteur est incrémenté à chaque nouvelle exécution de l'algorithme de déchiffrement  
15 jusqu'à une valeur T.

91937397

Translation

## PATENT COOPERATION TREATY

## PCT

## INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference GEM0652	<b>FOR FURTHER ACTION</b> See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)	
International application No. PCT/FR00/00723	International filing date (day/month/year) 22 March 2000 (22.03.00)	Priority date (day/month/year) 26 March 1999 (26.03.99)
International Patent Classification (IPC) or national classification and IPC H04L 9/30		
Applicant GEMPLUS		

<p>1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.</p> <p>2. This REPORT consists of a total of <u>5</u> sheets, including this cover sheet.</p> <p><input checked="" type="checkbox"/> This report is also accompanied by ANNEXES, i.e., sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).</p> <p>These annexes consist of a total of <u>17</u> sheets.</p>
<p>3. This report contains indications relating to the following items:</p> <p>I <input checked="" type="checkbox"/> Basis of the report</p> <p>II <input type="checkbox"/> Priority</p> <p>III <input type="checkbox"/> Non-establishment of opinion with regard to novelty, inventive step and industrial applicability</p> <p>IV <input type="checkbox"/> Lack of unity of invention</p> <p>V <input checked="" type="checkbox"/> Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement</p> <p>VI <input type="checkbox"/> Certain documents cited</p> <p>VII <input type="checkbox"/> Certain defects in the international application</p> <p>VIII <input checked="" type="checkbox"/> Certain observations on the international application</p>

Date of submission of the demand 23 September 2000 (23.09.00)	Date of completion of this report 28 June 2001 (28.06.2001)
Name and mailing address of the IPEA/EP	Authorized officer
Facsimile No.	Telephone No.

# INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.

PCT/FR00/00723

## I. Basis of the report

### 1. With regard to the elements of the international application:\*

- ☐ the international application as originally filed
- ☒ the description:  
 pages 1-5, as originally filed  
 pages \_\_\_\_\_, filed with the demand  
 pages 6-17, filed with the letter of 12 March 2001 (12.03.2001)
- ☒ the claims:  
 pages \_\_\_\_\_, as originally filed  
 pages \_\_\_\_\_, as amended (together with any statement under Article 19  
 pages \_\_\_\_\_, filed with the demand  
 pages 1-15, filed with the letter of 12 March 2001 (12.03.2001)
- ☐ the drawings:  
 pages \_\_\_\_\_, as originally filed  
 pages \_\_\_\_\_, filed with the demand  
 pages \_\_\_\_\_, filed with the letter of \_\_\_\_\_
- ☐ the sequence listing part of the description:  
 pages \_\_\_\_\_, as originally filed  
 pages \_\_\_\_\_, filed with the demand  
 pages \_\_\_\_\_, filed with the letter of \_\_\_\_\_

### 2. With regard to the language, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.

These elements were available or furnished to this Authority in the following language \_\_\_\_\_ which is:

- ☐ the language of a translation furnished for the purposes of international search (under Rule 23.1(b)).
- ☐ the language of publication of the international application (under Rule 48.3(b)).
- ☐ the language of the translation furnished for the purposes of international preliminary examination (under Rule 55.2 and/or 55.3).

### 3. With regard to any nucleotide and/or amino acid sequence disclosed in the international application, the international preliminary examination was carried out on the basis of the sequence listing:

- ☐ contained in the international application in written form.
- ☐ filed together with the international application in computer readable form.
- ☐ furnished subsequently to this Authority in written form.
- ☐ furnished subsequently to this Authority in computer readable form.
- ☐ The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.
- ☐ The statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.

### 4. ☐ The amendments have resulted in the cancellation of:

- ☐ the description, pages \_\_\_\_\_
- ☐ the claims, Nos. \_\_\_\_\_
- ☐ the drawings, sheets/fig \_\_\_\_\_

### 5. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).\*\*

\* Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report since they do not contain amendments (Rule 70.16 and 70.17).

\*\* Any replacement sheet containing such amendments must be referred to under item 1 and annexed to this report.

**V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement****1. Statement**

Novelty (N)	Claims	1-15	YES
	Claims		NO
Inventive step (IS)	Claims		YES
	Claims	1-15	NO
Industrial applicability (IA)	Claims	1-15	YES
	Claims		NO

**2. Citations and explanations****1. Reference is made to the following documents:**

**D1: Paul Kocher et al.: 'Introduction to Differential Power Analysis and Related Attacks'**  
<URL: <http://www.cryptography.com/dpa/technical/index.html>>, pages 1-8, XP002132318 San Francisco, CA, USA

**D2: Menkus B: 'Two important data encryption structures reported broken in record times'**  
EDPACS, Jan. 1999, Auerbach Publications, USA,  
vol.26, no.7, pages 15-18, XP000884687  
ISSN:0736-6981

2. Document D2 (Menkus) discloses the concept on which the independent claims are based. Indeed, said document discloses (see, in particular, page 18) a countermeasure method based on incorporating random calculations into the integrated chip software, or the modification to the order of operations carried out by said software.

The fact that in independent Claims 1, 6 and 11, said random calculations are implemented within the

framework of elliptic curve algorithms, which are well known *per se*, does not contribute any advantage that would go beyond this basic concept, and said feature, while rendering the subject matter of said claims novel, does not therefore involve an inventive step.

3. Since the subject matter of the independent claims is novel, the same is true of the dependent claims. However, said claims do not contain any additional features that would render the subject matter thereof inventive.
4. It should be noted that document D1 is also considered to be very relevant.

**VIII. Certain observations on the international application**

The following observations on the clarity of the claims, description, and drawings or on the question whether the claims are fully supported by the description, are made:

The use of the French expression "a first alternative consists in that" in Claim 2, and "a second alternative consists in that" in Claim 3 renders the subject matter of said claims ambiguous (PCT Article 6).

**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record**

## **BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☒ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: \_\_\_\_\_

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**